Association for Computing Machinery

*Advancing Computing as a Science & Profession*

**NEWS RELEASE**

**Contact:** Jim Ormond
ACM
212-626-0505
ormond@acm.org

**WHAT CYBERSECURITY SKILLS DO COMMUNITY COLLEGE STUDENTS NEED TO GET A JOB?**

***ACM Releases Curriculum Guidelines Outlining What Competencies Students in Two-Year Programs Should Have Upon Graduation***

**New York, NY, March 10, 2020** – According to the US Bureau of Labor Statistics, demand for information security analysts is expected to grow by 32% between 2018 and 2028−outpacing growth in many other professions. Cybersecurity professionals work in every imaginable industry, including banking and finance, technology-focused companies, government institutions and the military, and non-profit organizations such as hospitals.

Community colleges and related two-year programs have emerged as important venues for information security training. According to the American Association of Community Colleges, 40% of all undergraduates in the United States are enrolled in two-year colleges. A shared goal of college administrators, faculty, and industry leaders has been to ensure that students in two-year programs receive the appropriate training that will allow them to continue their education toward obtaining baccalaureate degrees, or secure information security jobs immediately after earning their associate degree−and prosper in those jobs.

To this end, the Association for Computing Machinery's Committee for Computing Education in Community Colleges (CCECC) recently released Cybersecurity Curricular Guidance for Associate Degree Programs (Cyber2yr2020), a report outlining competencies and learning outcomes for those pursuing careers in information security.

"With growing cyber threats in both the private and public sectors, continuous curriculum development is critical because the nature of the threats continuously evolves, thus increasing the knowledge and skill sets needed by the cybersecurity workforce," explains Cyber2yr2020 Task Group Chair Cara Tang of Portland Community College. "Providing guidance for cybersecurity programs at community colleges is critical for a number of reasons. As drivers of local economic development, community colleges are among the first places employers look for new hires. We want to ensure that we are serving students by

giving them the specific skills that the workforce demands−or adequately preparing them to continue their studies at four-year institutions."

Cyber2yr2020 builds upon Cybersecurity Curricular Guidelines (CSEC 2017), an earlier report compiled by ACM and other leading organizations geared towards baccalaureate programs. The new report follows CSEC 2017 in outlining eight core areas that cybersecurity students should be proficient in. These areas include Data Security, Software Security, Component Security, Connection Security, System Security, Human Security, Organizational Security, and Societal Security. While keeping the areas of the earlier report intact, in the new report, "domain" and "subdomain" are preferred terms to "knowledge area" and "knowledge unit," that were used in the earlier report, since the focus on the new curricula is on competencies and outcomes, which go beyond knowledge to also include skills and dispositions in context.

The Cyber2yr2020 Curricular Guidance report also lists important Cross-Cutting Concepts such as confidentiality, integrity, availability, risk, adversarial thinking, and system thinking that help students explore the connections among the eight core areas and reinforce the importance of a security mindset throughout all core areas. In addition to essential competencies that students should have proficiency in, Cyber2yr2020 also lists supplemental competencies, to reflect the broad variety of associate degree cybersecurity programs across the US.

The 10-member Cyber2yr2020 task force that developed the report is made up of community college educators with varying expertise in cybersecurity from community and technical colleges across the United States. In addition to Chair Cara Tang, the Cyber2Yr2020 task force includes Cindy Tucker, Bluegrass Community and Technical College, Lexington, KY; Christian Servin, El Paso Community College, El Paso, TX; Markus Geissler, Cosumnes River College, Sacramento, CA; Melissa Stange, Lord Fairfax Community College, Middletown, VA; Nancy Jones, Coastline Community College, Garden Grove, CA; James Kolasa, Bluegrass Community and Technical College, Lexington, KY; Amelia Phillips, Highline College, Des Moines, WA; Lambros Piskopos, Wilbur Wright College, Chicago, IL; and Pam Schmelz, Ivy Tech Community College, Columbus, IN.

**About CCECC**

The ACM Committee for Computing Education in Community Colleges (CCECC) serves and supports community and technical college educators in all aspects of computing education. Chartered in 1991 as a standing committee of the ACM Education Board, the CCECC is concerned with computing education at associate-degree granting colleges in the United States and similar post-secondary institutions throughout the world. The Committee engages in curriculum and assessment development, community building, as well as advises on public policy and advocacy in service to this sector of higher education.

**About ACM**

ACM, the Association for Computing Machinery**,** is the world's largest educational and scientific computing society, uniting computing educators, researchers and professionals to inspire dialogue, share resources and address the field's challenges. ACM strengthens the computing profession's collective voice through strong leadership, promotion of the highest standards, and recognition of technical excellence. ACM supports the professional growth of its members by providing opportunities for life-long learning, career development, and professional networking.

###